

In the claims

---

1 1. (amended) A system for maintaining security in a distributed computing  
2 environment, comprising:  
3 a policy manager for managing a security policy; and  
4 an application guard for managing access to securable components as specified by  
5 the security policy;  
6 wherein said securable components are separate and distinct from said security  
7 policy.

1 2. (amended) The system of claim 1 further comprising a management station for  
2 constructing and editing the security policy.

1 3. The system of claim 2, wherein said policy manager further comprises a  
2 distributor for distributing the security policy to a client.

1 4. The system of claim 2, wherein said policy manager further comprises a  
2 distributor for distributing a customized local policy based on the security policy to a  
3 client.

1 5. The system of claim 4, wherein said policy manager further comprises a logger  
2 for recording and tracking authorization events that occur through the application guard.

1 6. The system of claim 4, wherein the policy manager further comprises a database  
2 management system for maintaining the security policy.

1 7. The system of claim 4, wherein the customized local policy is optimized.

[Claim 8 cancelled previously]

1 9. (amended) The system of claim 1, wherein said system further comprises a  
2 plurality of clients, said policy manager manages and distributes a customized local  
3 policy to each client, and each client includes at least one additional application guard for  
4 managing access to the securable components of that client as specified by each  
5 customized local policy.

1 10. The system of claim 1, wherein said application guard includes an application  
2 guard interface coupled to an application for requesting access to the securable  
3 components, and at least one authorization engine for evaluating requests from the  
4 application guard interface as specified by a customized local policy based on the  
5 security policy.

B' 1 11. The system of claim 10, wherein said application guard interface is located on a  
2 client, and said at least one authorization engine and said customized local policy are  
3 located on a client server.

1 12. The system of claim 1, wherein the security policy is defined by a policy language  
2 to grant or deny access to the securable components for a particular user.

1 13. The system of claim 1 further comprising a policy loader for bulk loading the  
2 security policy onto the system.

1 14. The system of claim 1, wherein said policy manager includes a set of menu  
2 options to manage and distribute the security policy.

1 15. The system of claim 14, wherein said set of menu options include: navigate tree,  
2 analyze policy, edit policy, distribute policy, and view audit log.

[Claim 16 cancelled previously]

1 17. The system of claim 1, wherein the policy manager further includes a policy  
2 manager application guard for managing access to the policy manager as specified by a  
3 local administrative policy.

1 18. (amended) A system for controlling user access in a distributed computing  
2 environment, comprising:  
3 a global policy specifying access privileges of the user to securable components;  
4 a policy manager located on a server for managing and distributing to a client a  
5 local client policy based on the global policy, and  
6 an application guard located on the client for managing access to the securable  
7 components as specified by the local client policy.

B1  
1 19. (amended) The system of claim 18 further comprising at least one additional  
2 client, said policy manager further managing and distributing to each additional client a  
3 customized local policy based on the global policy, and comprising at least one additional  
4 application guard located on each additional client for managing access to the securable  
5 components as specified by the customized local policy.

1 20. The system of claim 18, wherein said policy manager comprises:  
2 a management station for constructing and editing the global policy; and  
3 a distributor for distributing the local policy to the client.

1 21. The system of claim 20, wherein said policy manager further comprises a  
2 database management system for maintaining the global policy.

1 22. The system of claim 18, wherein said policy manager further comprises a logger  
2 for recording and tracking authorization events that occur through the application guard.

[Claim 23 cancelled previously]

1 24. The system of claim 18, wherein the global policy is defined by a policy language  
2 to grant or deny access to the securable components for a particular user.

1 25. The system of claim 18, wherein said system is scalable by further comprising a  
2 plurality of clients, said policy manager further managing and distributing a customized  
3 local policy to each client, and at least one additional application guard located on each  
4 client for managing access to the securable components as specified by each customized  
5 local policy.

1 26. The system of claim 18, wherein said application guard includes an application  
2 guard interface coupled to an application for requesting access to the securable  
3 components, and at least one authorization engine for evaluating requests from the  
4 application guard interface as specified by the local client policy.

B<sup>1</sup>  
1 27. The system of claim 18 further comprising a policy bulk loader for bulk loading  
2 the global policy onto the system.

1 28. The system of claim 18, wherein the local client policy is optimized.

[Claim 29 cancelled previously]

1 30. The system of claim 18, wherein the policy manager further includes a policy  
2 manager application guard for managing access to the policy manager as specified by a  
3 local administrative policy.

1 31. A system for authorization that provides access to securable components for a  
2 user, comprising:  
3 a policy specifying access privileges of the user to the securable components;  
4 an application guard; and  
5 a processor coupled to said system, said processor executing said application  
6 guard to manage access to the securable components.

1 32. The system of claim 31 further including an audit log for recording and tracking  
2 each authorization event that occurs through the application guard.

[Claim 33 cancelled previously]

1 34. The system of claim 31, wherein said application guard comprises an application  
2 guard interface connected to an application for managing access to the securable  
3 components in said application.

[Claim 35 cancelled previously]

B1  
1 36. The system of claim 31, wherein said application guard includes an application  
2 guard interface coupled to an application for requesting access to the securable  
3 components, and at least one authorization engine for evaluating requests from the  
4 application guard interface as specified by a customized local policy based on the policy.

1 37. The system of claim 36, wherein said application guard interface is located on a  
2 client, and said at least one authorization engine and said customized local policy are  
3 located on a client server.

1 38. A system for managing security in a distributed computing environment,  
2 comprising:  
3 a policy manager; and  
4 a processor coupled to said system, said processor executing said policy manager  
5 to manage and distribute a customized local policy based on a global  
6 policy to a client.

1 39. The system of claim 38, wherein said policy manager comprises a management  
2 station for constructing and editing the global policy.

1 40. The system of claim 39, wherein said policy manager further comprises a  
2 distributor for distributing the customized local policy to the client.

1 41. The system of claim 38, wherein said policy manager further comprises a logger  
2 for recording and tracking authorization events that are received from the client.

1 42. The system of claim 38, wherein said global policy specifies access privileges of  
2 at least one user to securable components.

1 43. The system of claim 38, wherein the policy manager comprises a database  
2 management system for maintaining the global policy.

B1  
1 44. The system of claim 38, wherein the global policy is defined by a policy language  
2 to grant or deny access to securable components for a particular user.

1 45. The system of claim 38, wherein said policy manager includes a set of menu  
2 options to manage and distribute the customized local policy.

1 46. The system of claim 38, wherein the customized local policy is optimized.

1 47. The system of claim 38, wherein the policy manager further includes a policy  
2 manager application guard for managing access to the policy manager as specified by a  
3 local administrative policy.

1 48. (amended) A method for maintaining security in a distributed computing  
2 environment, comprising the steps of:  
3 managing a policy by using a policy manager to specify access privileges of a  
4 user to securable components; and  
5 distributing the policy to a client having an application guard which manages  
6 access to the securable components as specified by the policy.

1 49. The method of claim 48, further including the step of recording authorization  
2 events that occur through the application guard after distributing the policy.

[Claim 50 cancelled previously]

1 51. (amended) A method for maintaining security on a client in a distributed  
2 computing environment, comprising the steps of:  
3 using an application guard interface for issuing an authorization request for a user  
4 to gain access to securable components located on the client;  
5 using the application guard to evaluate the authorization request and thereby  
6 determine if the authorization request is valid or invalid; and  
7 allowing access to the user via the application guard if the evaluated authorization  
8 request was valid, and denying access to the user via the application guard  
9 if the authorization request was invalid.

1 52. The method of claim 51, after evaluating the authorization request, further  
2 including the step of recording the authorization request in an audit log.

1 53. (amended) A computer-readable medium comprising program instructions for  
2 maintaining security in a distributed computing environment by performing the steps of:  
3 managing a policy by using a policy manager to specify access privileges of a  
4 user to securable components;  
5 distributing the policy using the policy manager to a client having an application  
6 guard, whereby the application guard manages access to the securable  
7 components as specified by the policy; and  
8 executing said policy manager with a processor to manage and distribute the  
9 policy.

B1

1 54. A computer-readable medium comprising program instructions for maintaining  
2 security on a client in a distributed computing environment by performing the steps of:  
3 constructing and issuing an authorization request for a user to access to securable  
4 components located on the client using an application guard;  
5 evaluating the authorization request using the application guard to determine if  
6 the authorization request is valid or invalid;  
7 allowing access to the user via the application guard if the evaluated authorization  
8 request was valid, and denying access to the user via the application guard  
9 if the authorization request was invalid; and  
10 executing said application guard with a processor to automatically maintain  
11 security on the client.

1 55. A system for maintaining security in a distributed computing environment,  
2 comprising:  
3 means for managing a policy using a policy manager by specifying access  
4 privileges of a user to securable components;  
5 means for distributing the policy using the policy manager to a client having an  
6 application guard, whereby the application guard manages access to the  
7 securable components as specified by the policy; and  
8 means for executing the policy manager to manage and distribute the policy.



1 56. A system for maintaining security on a client in a distributed computing  
2 environment, comprising:  
3 means for constructing and issuing an authorization request for a user to access to  
4 securable components located on the client using an application guard;  
5 means for evaluating the authorization request using the application guard to  
6 determine if the authorization request is valid or invalid;  
7 means for allowing access to the user via the application guard if the evaluated  
8 authorization request was valid, and denying access to the user via the  
9 application guard if the authorization request was invalid; and  
10 means for executing said application guard to automatically maintain security on  
11 the client.

B<sup>1</sup>  
1 57. The system of claim 1 wherein the computer readable components are associated  
2 with an application and are stored on a computer readable medium.

1 58. A system for maintaining security in a distributed computing environment,  
2 comprising:  
3 a policy manager for managing a security policy; and  
4 an application guard for managing access to a transaction related with an  
5 application as specified by the security policy.

1 59. (amended) A system for managing and enforcing complex security requirements  
2 to protect computer systems against unauthorized access in a distributed computer  
3 network comprising:  
4 a policy manager located on a server for managing and distributing a policy to a  
5 client; and  
6 an application guard located on the client, acting to grant or deny access to  
7 various components of the client, as specified by the policy.

1 60. The system of claim 59 wherein the server is connected via a network to the  
2 client.

1 61. The system of claim 59 wherein the server is connected to many clients.

1 62. The system of claim 59 the server further comprising:

2 a central processing unit;

3 a Read-Only Memory (ROM);

4 a Random-Access Memory (RAM);

5 a non-volatile memory;

6 an input device; and

7 a display;

8 wherein the ROM, the RAM, non-volatile memory, input device and display are

9 connected via a bus.

B1  
1 63. The system of claim 59 wherein the policy manager is a program located on a  
2 server in non-volatile memory.

1 64. The system of claim 59 wherein the client contains a program stored in non-  
2 volatile memory for granting or denying access to various components or resources of the  
3 client, as specified by the policy distributed from the server.

1 65. (amended) The system of claim 59 wherein the server includes a non-volatile  
2 memory storing the policy manager that specifies the security requirements for  
3 applications and database objects;  
4 said policy contains security rules that describe at least one constraint that  
5 constrains  
6 which applications a particular user can access and  
7 which objects within an application a user can access.

1 66. (amended) The system of claim 65 wherein the policy manager allows the  
2 administrator to choose whether the constraints are affected by any of  
3 time,  
4 geography, and  
5 external events.

1 67. The system of claim 59 wherein the policy is capable of constraining access to  
2 applications and operations within applications.

1 68. The system of claim 59 wherein the policy is organized into groups and  
2 hierarchies.

B1  
1 69. The system of claim 59 wherein the policy includes access rules, which include:  
2 a grant rule that grants a privilege to a subject on an object under a first constraint;  
3 and  
4 a deny rule that denies a privilege to a subject on an object under a second  
5 constraint.

1 70. The system of claim 59 the policy manager further comprises  
2 a management station program to operate the policy manager,  
3 a distributor program to distribute local client policies to clients,  
4 a logger program to track authorization requests, and  
5 a database management system (DBMS) to maintain policy data files.

1 71. The system of claim 59 wherein the policy manager further comprises:  
2 an audit log data file to record authorization requests;  
3 an optimized policy data file;  
4 an enterprise policy data file;  
5 an administrative policy data file; and  
6 a local administrative policy data file.

1 72. The system of claim 59 wherein the policy manager is located within non-volatile  
2 memory.

1 73. The system of claim 59 wherein the policy manager allows system users to  
2 implement,  
3 analyze,  
4 edit and  
5 update  
6 a centrally-managed policy.

B1  
1 74. The system of claim 59 wherein the policy includes at least one policy rule  
2 comprising:  
3 1) an object that is to be protected;  
4 2) an access right or privilege;  
5 3) a global or local user to which the privilege applies; and  
6 4) conditions under which the privilege is granted or denied, wherein the user is  
7 given a choice of types of conditions including  
8 whether to use built-in access criteria wherein the user can select  
9 whether to use time of day and  
10 whether to use location,  
11 and  
12 whether to use custom-defined access criteria.

1 75. The system of claim 59 wherein the policy manager comprises a Graphical User  
2 Interface (GUI) that provides at least a user-friendly set of menu options or management  
3 services to fully operate the policy manager and control programs that perform at least  
4 navigation,  
5 searching,  
6 distribution,  
7 editing,  
8 querying, and  
9 log viewing.

B1  
1 76. The system of claim 59 wherein the policy manager comprises an Application  
2 Programming Interface (API) that at least allows programs to perform the same functions  
3 as a human operator.

1 77. A system comprising a computer having a security policy that includes at least  
2 one or more components having at least:  
3 an object,  
4 a subject,  
5 a privilege, and  
6 a condition.

1 78. The system of claim 77 wherein each object can be an application or an operation  
2 within an application.

1 79. The system of claim 77 wherein the object is capable of being set to be at least  
2 any of:  
3 an application,  
4 a method,  
5 a web page,  
6 a database table  
7 a file, and  
8 one or more menu items in a graphical user interface.

1 80. The system of claim 77 wherein the object can be organized into at least an object  
2 hierarchy such that:  
3 if a user is granted a certain privilege on a parent object, then that user is  
4 automatically granted the privilege on all the children objects, and  
5 if the user is denied a certain privilege on a parent object, then that user is denied  
6 the privilege on all the children objects.

1 81. The system of claim 77 wherein the privilege is capable of being inherited from a  
2 parent to a child object.

1 82. The system of claim 77 wherein the subject is capable of being set to be at least  
2 any of:  
3 a user and  
4 a role containing one or more users, who can at least  
5 access a protected object, and  
6 have access to at least some information in the system.

1 83. The system of claim 77 wherein the subject is capable of being a user that can be  
2 chosen to be either internal or external to a system.

1 84. The system of claim 77 wherein the object comprises a list that is capable of  
2 containing one or more users authorized to access the object who can log on to the object  
3 and be authenticated by the object through an external authentication server.

1 85. The system of claim 77 wherein the system is capable of having the subject be a  
2 user who at least:  
3 can be maintained separately by one or more components each of which can be an  
4 object or directory server; and  
5 can be extracted from said one or more components to synchronize the  
6 components thereby maintaining their access current.

1 86. The system of claim 77 wherein components comprise an alias-user who at least  
2 inherits all privileges of a user under certain conditions, thereby facilitating authorization  
3 management by providing fine granularity of control on propagation of a privilege.

1 87. The system of claim 86 wherein the system is capable of having the alias-user be  
2 created to perform a job function while the user is absent, and inheritance of the privilege  
3 takes effect only when the user is absent.

1 88. The system of claim 77 wherein a user of the object is capable of being defined to  
2 be local to the object.

1 89. The system of claim 77 wherein a user can be at least a global user mapped to a  
2 set of local users having at least one local user per object.

1 90. The system of claim 77 wherein the privilege defines at least one kind of access  
2 that is allowed to the object and includes at least one right to perform a particular action  
3 on the object.

1 91. The system of claim 77 wherein the privilege is capable of including at least  
2 a right to execute an application,  
3 a right to download a web page,  
4 a right to query a database table, or  
5 a right to view a menu item.

1 92. The system of claim 77 wherein the component is capable of being assigned to be  
2 a wild card that is capable of being used at least as a privilege, object, or subject.

1 93. The system of claim 77 further comprising an access request that includes at least:  
2 a privilege,  
3 an object, and  
4 a subject;  
5 wherein the access request is used by at least a subject to request authorization of  
6 at least a privilege on at least an object.

1 94. The system of claim 93 wherein the access request at least:  
2 matches a grant rule if the privilege, object, and subject match those in the rule,  
3 and the constraint in the rule is met; and  
4 matches a deny rule if the privilege, object, and subject match those in the rule,  
5 and the constraint in the rule is not met.

1 95. The system of claim 77 wherein an access request is at least:  
2 denied if  
3 there is a deny rule matching a request, or  
4 there are no access rules matching the request; and  
5 granted if there are no deny rules matching the request and there is a grant rule  
6 matching the request.



1 96. (amended) The system of claim 77 wherein conditions comprise constraints and  
2 the system has at least facilities for defining constraints as expressions formed from  
3 operators including at least NOT, AND, and OR.

1 97. The system of claim 77 wherein conditions at least:  
2 are constraints on when the object or the subject can be accessed,  
3 specify requirements on when the access rule is applicable, and  
4 contain options that can be set to be dependent on properties of the object or the  
5 subject.

1 98. The system of claim 77 wherein the system further comprises facilities for  
2 expressing constraints as at least:  
3 1) relational operations on integers;  
4 2) relational operations on strings; and  
5 3) set operations.

1 99. The system of claim 77 wherein the system further comprises facilities that allow  
2 the user to define conditions.

1 100. The system of claim 77 wherein the system includes an Application Programming  
2 Interface (API) for invoking user-supplied code to evaluate user-defined functions.

1 101. (amended) A system comprising a computer having a security policy that  
2 includes at least one or more components having at least a set of privileges that includes  
3 at least one privilege that is capable of at least:  
4 being granted to a user explicitly; and  
5 being granted to a role which is granted to the user.

1 102. (amended) The system of claim 101 wherein:  
2 the role is a named group of privileges containing at least one privilege that are  
3 granted to at least one user or to at least one other role; and  
4 the at least one user granted the role is a member of the role.

1 103. The system of claim 101 wherein the members of a role automatically inherit all  
2 the privileges granted or denied to the role.

1 104. (amended) The system of claim 101 wherein roles are organized into a role  
2 hierarchy, where parent roles are granted to children roles such that:  
3 if a parent role is granted a privilege, then the children roles are automatically  
4 granted the privilege; and  
5 if a parent role is denied a privilege, then the children roles are automatically  
6 denied the privilege.

1 105. The system of claim 101 wherein roles of an object may be defined as being local  
2 to that object.

1 106. The system of claim 101 wherein the role is at least a global role mapped to at  
2 least a set of local roles, having at least one role per object.

1 107. The system of claim 101 wherein the system further comprises more than one  
2 role, two of which have memberships that are mutually exclusive with respect to one  
3 another.

1 108. (amended) A security system comprising a policy manager located on a computer  
2 system that includes at least:  
3 a management console or station;  
4 a database management system;  
5 an audit facility; and  
6 a distributor.

1 109. (amended) The system of claim 108 wherein the management station comprises a  
2 Graphical User Interface (GUI) for users to create and customize rules by system users.

1 110. The system of claim 108 wherein the management station supports concurrent  
2 rule development by multiple users.

B<sup>1</sup>  
1 111. (amended) The system of claim 108 wherein the management station includes an  
2 application guard to allow only authorized administrators to operate the management  
3 station based on at least a local administrative policy which provides a set of policy rules  
4 specifying which users are authorized to access the management station.

1 112. (amended) A security system comprising:  
2 at least one application guard that is stored on a computer readable medium and  
3 that guards a protected application by preventing unauthorized transactional access to at  
4 least a portion of said application.

1 113. A security system comprising:  
2 an application guard located within non-volatile memory that is designed to reside  
3 along with each protected application and supports transactional access control by  
4 allowing an application to detect an authorization service and to make authorization  
5 requests at each user interaction, data request, and business-level transaction.

1 114. (amended) The security system of claim 113 further comprising a distributor  
2 capable of distributing the application guard to clients located throughout an enterprise.

1 115. (amended) The system of claim 113 wherein the application guard is coupled to  
2 the application through an application programming interface (API) or authorization  
3 library that allows the application to request authorization services as needed through an  
4 application guard interface.

1 116. (amended) The system of claim 113 further comprising  
2 an authorization engine that processes an authorization request;  
3 a checker that parses local client policy and stores the parsed local client policy in  
4 Random Access Memory (RAM); and  
5 an evaluator that evaluates the authorization request with the parsed local client  
6 policy in RAM to determine whether the authorization request should be granted or  
7 denied.

1 117. The system of claim 113 wherein the authorization engine comprises plug-ins that  
2 at least allow for additional capabilities to process and evaluate authorization requests  
3 based on customized code.

1 118. (amended) The system of claim 113 further comprising a logger where at least:  
2 each authorization request is recorded in an audit log; and  
3 each authorization request made at a location remote from the logger is  
4 transmitted via a communication interface to the logger.

1

2

1 119. The system of claim 113 wherein the system is capable of implementing at least:  
2 the application guard locally to the application; and  
3 the application guard as a remote authorization service through a remote  
4 procedure call to another server.

1 120. A security system comprising:  
2 at least one application guard stored on a computer readable non-volatile memory  
3 medium that is designed to reside along with each protected application and  
4 guards a protected application by preventing unauthorized transactional  
5 access, and  
6 supports transactional access control by allowing an application to detect  
7 an authorization service and to make authorization requests at each user  
8 interaction, data request, and business-level transaction;  
9 wherein  
10 the application guard is integrated into the application through an  
11 application programming interface (API) or authorization library that allows the  
12 application to request authorization services as needed through an application  
13 guard interface, and  
14 the system is capable of implementing the application guard locally to the  
15 application and is capable of implementing the application guard as a remote  
16 authorization service through a remote procedure call to another server.

1 121. A computer readable storage medium having stored thereon a method for  
2 maintaining security in a distributed computing environment comprising the steps of:  
3 managing a security policy via a policy manager; and  
4 managing access via an application guard to a transaction related with an  
5 application as specified by the security policy.

- 1 122. A method for maintaining security in a distributed computing environment,  
2 comprising:  
3 managing a security policy via a policy manager; and  
4 managing access via an application guard to a transaction referenced by an  
5 application as specified by the security policy.
- 1 123. (amended) A method of using a security system comprising:  
2 using a management station, including a communication interface, to create or  
3 modify a policy rule; and  
4 distributing the policy rule to appropriate clients via the communication interface.
- 1 124. (amended) The method of claim 123 further comprising reviewing and  
2 reconstructing the policy rules via a parser to make sure that the policy rules are  
3 syntactically and semantically correct according to a predefined policy language.
- 1 125. (amended) The method of claim 123 further comprising determining via a differ-  
2 program the changes that were made to optimize the policy, and wherein the step of  
3 distributing then distributes only the changed policy rules or local client policy to the  
4 appropriate application guards, which enforce access control to local applications and  
5 data.
- 1 126. The method of claim 123 wherein each application guard has its own specific  
2 local client policy.
- 1 127. The method of claim 123 further comprising optimizing via the distributor an  
2 administrative policy into an optimized administrative policy or local administrative  
3 policy for use with an application guard in the management station.

1 128. (amended) A method of distributing at least one security policy rule comprising:  
2 passing the policy rule through at least  
3 a DataBase (DB) layer and  
4 an Open DataBase Connectivity (ODBC) layer;  
5 and  
6 storing the policy rule as an enterprise policy.

1 129. The method of claim 128, wherein:  
2 the DB layer formats the policy rules into standard database storage tables, and  
3 the ODBC provides a common interface to various vendor-specific databases.

B1  
1 130. The method of claim 128 wherein the distribution occurs through the ODBC layer  
2 and a communication interface.

1 131. The method of claim 128 further comprising passing the enterprise policy to a  
2 distributor.

1 132. The method of claim 128 further comprising determining via an optimizer  
2 program within the distributor which application guard needs to receive the policy rules.

1 133. A method of configuring a security system comprising:  
2 installing a policy manager on a server including  
3 installing  
4 a management station,  
5 a distributor,  
6 a logger, and  
7 a DataBase Management System (DBMS);  
8 entering a set of policy rules  
9 installing application guards and local client policies onto client systems; and  
10 registering plug-ins into the application guards to allow for additional capabilities  
11 in order to process authorization requests based on customized code.

B/ 1 134. The method of claim 133 wherein the step of entering includes presenting an  
2 administrator with the choice of whether to use a policy loader or a management station  
3 to enter the policy rules.

1 135. (amended) The method of claim 133 wherein  
2 if the administrator chooses to use the management station, then the step of  
3 entering includes using an edit function to enter the policy rules, and  
4 if the administrator chooses to use the policy loader, then the step of entering  
5 includes  
6 entering the policy rules into a file, and  
7 passing the file to the policy loader.



1 136. (amended) A method of managing policy under management services in a  
2 management station comprising:  
3 an authorized administrator logging into a policy manager;  
4 the authorized administrator choosing either administrative mode to manage  
5 administrative policy or enterprise mode to manage enterprise policy;  
6 presenting the administrator with menu options including  
7 navigate tree,  
8 analyze policy,  
9 edit policy,  
10 distribute policy,  
11 view audit log to allow the administrator to view and track authorization  
12 requests that have occurred at an application guard connected to a system, and  
13 exit.

1 137. (amended) The method of claim 136 wherein the menu option navigate tree  
2 provides a set of edit options for an administrator that include to  
3 add,  
4 delete, and  
5 modify features; and  
6 wherein the administrator is presented with a choice of features on a server and on  
7 a client.

1 138. (amended) The method of claim 136 wherein the features to which the  
2 administrator can apply the edit policy option include  
3 global users,  
4 global roles,  
5 directories,  
6 local roles,  
7 local users,  
8 applications,  
9 application guards, and  
10 declarations.

1 139. (amended) The method of claim 136 wherein the menu option analyze policy  
2 allows an authorized user to analyze and view rules and policies within the enterprise  
3 policy.

B1  
1 140. (amended) The method of claim 136 wherein the administrator is presented with  
2 options  
3 to search rules, and  
4 to query policy.

1 141. The method of claim 140 wherein if search rules is selected, the administrator is  
2 presented with options of searching grant rules and all the deny rules pertaining to a  
3 particular user.

1 142. The method of claim 140 wherein if query policy is selected, a search can be  
2 made on who is granted or denied what privilege on which objects under what conditions.

1 143. The method of claim 140 wherein the menu option edit policy presents an  
2 authorized user with the option to add, delete, and modify enterprise policy features.

1 144. (amended) The method of claim 143 wherein the features that may be edited  
2 include  
3 a rule set,  
4 access,  
5 a privilege,  
6 an object,  
7 a user  
8 a role, and  
9 an attribute.

1 145. The method of claim 136 wherein the menu option distribute policy includes  
2 distributing the new features of a newly entered or modified enterprise policy to  
3 appropriate application guards.

B1  
1 146. (amended) The method of claim 136 wherein upon selecting the distribute policy  
2 option  
3 a distributor optimizes enterprise policy;  
4 a differ program computes a difference between a newly optimized policy and a  
5 formerly optimized policy;  
6 the newly optimized policy is then published as optimized policy in DBMS;  
7 only the changed portions of the newly optimized policy are committed to an  
8 appropriate application guard;  
9 the application guard receives the changed portions of the newly optimized  
10 policy;  
11 the application guard merges the received changed portions into local client  
12 policy; and  
13 the local client policy is activated to work with the application guard.

1 147. (amended) A method of granting client access authorization comprising:  
2 using an application guard that includes at least  
3 requesting access to a software securable component associated with an  
4 application protected by the application guard, wherein the application guard  
5 constructs and issues an authorization request, and  
6 evaluating the authorization request via the application guard according to  
7 its local client policy to determine whether to allow or deny the authorization  
8 request; and  
9 an audit records the authorization request in an audit log;  
10 wherein  
11 if there is an error in the authorization request, or if the request is  
12 not valid, then access is denied;  
13 if the authorization request is valid, then a determination is made  
14 whether access should be granted, and  
15 if the evaluated authorization request does not deny access,  
16 then access is allowed, and  
17 if the evaluated authorization request denies access, then  
18 access is denied.

1 148. (amended) The method of claim 147 wherein evaluating the authorization request  
2 includes an evaluator searching deny rules in a local policy, and  
3 if the evaluator finds a deny rule, then an evaluation is performed on any  
4 constraints on the deny rule,  
5 if the evaluation finds a presently valid constraint on the deny rule,  
6 then access is denied, and  
7 if the evaluation finds that all constraints on the deny rule are not  
8 presently valid, then a search for a grant rule is performed;  
9 and  
10 if no deny rules are found, then a search for a grant rule is performed;  
11 wherein after a search for a grant rule  
12 if no grant rule is found that would allow access for the user, then  
13 access is denied, and  
14 if a grant rule is found, then an evaluation is performed on any  
15 constraints in the grant rule wherein  
16 if the evaluated constraint is presently valid, then access is  
17 allowed, and  
18 if the evaluated constraint is not presently valid, then access  
19 is denied.

1 149. A method for securing a computer system, comprising:  
2 guarding a protected application by using an application guard to prevent  
3 unauthorized transactional access.

1 150. (amended) A method for providing a security system, comprising:  
2 providing at least one application guard that is storable on a computer readable  
3 medium and guards a protected application by preventing unauthorized transactional  
4 access to at least a component associated with the application.

1 151. (amended) A method for updating a security system, comprising:  
2 updating a set of policy rules containing at least one policy rule in a central  
3 location;  
4 generating changes to the set of policy rules resulting from the updating step; and  
5 distributing the changes.

1 152. The method of claim 151 wherein the policy rule contains entitlement information  
2 related to at least one resource.

1 153. The method of claim 151 wherein the policy rules are stored in a database table.

B1  
1 154. (amended) A method for establishing a security system, comprising:  
2 establishing a set of policy rules containing at least one policy rule in a central  
3 location; and  
4 distributing the set of policy rules for enforcement.

1 155. The method of claim 154 wherein the policy rule contains entitlement information  
2 related to at least one resource.

3 156. The method of claim 154 wherein the policy rules are stored in a database table.

---